REMARKS

Applicants reply to the Office Action mailed on October 10, 2006 within two months. Thus, Applicants request an Advisory Action, if necessary. Claims 1-16 and 18-21 were pending and the Examiner rejects claims 1-16 and 18-21. Support for the amendments may be found in the originally-filed specification, claims, and figures. No new matter has been introduced by these amendments. Reconsideration of this application is respectfully requested.

Applicants respectfully assert that the subject matter of the various claims was commonly owned at the time the inventions covered therein were made and therefore, Applicants have complied with 37 C.F.R. § 1.56.

DOUBLE PATENTING REJECTION

Claims 1 and 20 stand provisionally rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1 and 3 of copending App. No. 10/710,307. Applicants assert that the amendments to claims 1 and 20 render this provisional rejection moot and respectfully request withdrawal of the rejection.

35 U.S.C. § 103 REJECTIONS

Claims 1-7, 9-15, 18 and 20-21 stand rejected under 35 U.S.C. § 103 (a) as being unpatentable over Black, U.S. Pub. No. 2005/0122209 ("Black") in view of in view of Hohle et al, U.S. Pat. No. 6,101,477 ("Hohle"). Claims 8, 9, 16, and 21 stand rejected over Black/Hohle in view of de Sylva, U.S. Pub. No. 2005/0098621 ("de Sylva"). Claims 8, 9, 16, 18, and 21 stand rejected over Black/Hohle in view of Moebs, U.S. Pub. No. 2005/0065872 ("Moebs"). Claim 12 stands rejected over Black/Hohle in view of Jensen et al. U.S. Pub. No. 2005/0165684 ("Jensen"). Applicants respectfully traverse.

Applicants' amendment to independent claim 1 renders this rejection moot. While Black, Hohle, de Sylva and Moebs disclose various biometric or smartcard technologies useful in transactions, neither Black, Hohle, de Sylva, Moebs, nor any combination thereof, disclose or suggest a method including at least "generating data representing said proffered biometric sample; [and] using said data representing said proffered biometric sample as a variable in an encryption calculation to secure at least one of said user information, said smartcard information and transaction data," as recited in amended claim 1.

Accordingly, Applicants assert that claim 1 is patentable over the cited references. Claims 2-16 and 18-21 variously depend from claim 1 and contain all of the elements thereof, so Applicants assert that claims 2-16 and 18-21 are differentiated from the cited references at least for the same reasons as set forth above, in addition to their own respective features.

For example, neither Black, Hohle, de Sylva, Moebs, nor any combination of thereof, disclose or suggest at least a method for registering biometric information including "using said data representing said proffered biometric sample as at least one of a private key, a public key, and a message authentication code to facilitate transaction security measures" as recited in amended claim 5. Similarly, neither Black, Hohle, de Sylva, Moebs, nor any combination of thereof, disclose or suggest at least a method for registering biometric information including "using said data representing said proffered biometric sample in generating a message authentication code and as at least one of a private key and a public key" as recited in claim 6. Neither Black, Hohle, de Sylva, Moebs, nor any combination of thereof, disclose or suggest at least a method for registering biometric information including "using said data representing said proffered biometric sample to facilitate substantially simultaneous access to goods and initiation of authentication for a subsequent purchase of said goods," as recited in claim 13.

The amendments to the claims are supported in the specification by at least paragraphs [00331-00332]:

> [00331]   In another exemplary embodiment of the present invention, one or more biometric samples may be used to sign and/or encrypt information. For example, smartcard 100 and/or reader 2500 may be configured to receive a biometric sample from a user. The sample may then be digitized and used, for example, as a variable in an encryption calculation to secure data. If the user wants to retrieve the encrypted data, the user must submit the relevant biometric sample and have it authenticated by any of the methods described herein. Once the biometric sample is authenticated, the data will be decrypted for access.

> [00332]   Similarly, a biometric may be used as both a private key and a public key for encryption purposes. In one exemplary embodiment, an entity may use stored biometric sample information to encrypt data in a manner similar to a public key. The data may then be configured such that it is only accessible by a real biometric sample, for example, by a user proffering a

AXP No. 200501333   8

PAGE 9/11 * RCVD AT 12/8/2006 10:39:57 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-3/13 * DNIS:2738300 * CSID:602 382 6070 * DURATION (mm-ss):03-26

fingerprint sample at a reader. Upon verification of the real
biometric sample, the data may be decrypted and/or retrieved.

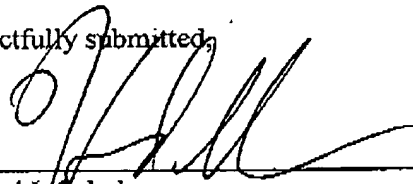Additional support is found in at least paragraphs [00138-00146, 00249, 00253, 00316, and 00320]

Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-16 and 18-21.

CONCLUSION

Applicants respectfully submit that the pending claims (21 total, 1 independent) are in condition for allowance. Reconsideration of the application is thus requested. **The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. 19-2814.** Applicants invite the Examiner to telephone the undersigned if the Examiner has any questions regarding this Reply or the application in general.

Respectfully submitted,

Dated: ___December 8, 2006___   By: _____

Howard I. Sobelman
Reg. No. 39,038

SNELL & WILMER L.L.P.
400 East Van Buren
One Arizona Center
Phoenix, Arizona 85004-2202
kdorius@swlaw.com
Telephone: (602) 382-6544
Facsimile: (602) 382-6070
1925816

AXP No. 200501333   10